eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Varredura passiva com Maltego**
  - ✓ O que é o Maltego
  - ✓ Tipos de licenças
  - ✓ Maltego vs Casefile
  - ✓ Definições Transforms x TDS
  - ✓ Edição Community vs Comercial
  - ✓ Colocando em Prática
    - ✓ Identificando DNS Servers
    - ✓ Identificando E-mails
    - ✓ Identificando MX Servers
    - ✓ Identificando IPs

Varredura Passiva: Maltego

Varredura Passiva: Maltego

O Maltego foi desenvolvido pela empresa PATERVA e roda em sistemas operacionais como Windows, Mac e Linux.

É capaz de determinar os relacionamentos entre links do mundo real, tais como:

- Pessoas
- Grupos de Pessoas (Redes Sociais)
- Companhias
- Organizações
- Web Sites

Intraestrutura interna como:

- Domínios
- Nomes de DNS
- Netblocks
- Endereços de IP

Varredura Passiva: Maltego

Há 2 versões do Maltego e uma ferramenta adicional (**CaseFile**)

A versão Community que é gratuita, porém, limitada
A versão Comercial, que tem um curso de $760

Também existe a ferramenta **CaseFile** que tem a função de analisar dados com a mesma flexibilidade dos gráficos do Maltego sem o uso de transformações.
É uma aplicação de inteligência visual que pode ser usado para determinar as relações e as ligações reais entre centenas de diferentes tipos de informações.

Você pode ligar pessoas e ações em suas ferramentas, vamos dar um exemplo:
Uma investigação criminal procura por traficantes, seus comparsas e sua hierarquia.
*Com o **Casefile**, você pode desenvolver e atribuir à investigação de modo gráfico toda a correlação entre eles.*

Varredura Passiva: Maltego

Na edição Community, você encontrará as seguintes limitações:

- *Máximo de 12 resultados por transform*
- *É necessário cadastro no site da Paterva*
- *As chaves de API expiram a cada 2 dias*
- *Executado em um servidor mais lento, que é compartilhado entre todos os usuários da comunidade*
- *A comunicação entre cliente e servidor não é criptografada*
- *Não possui atualização, até a próxima versão principal*
- *Não há suporte para usuários*
- *Só poderá efetuar a varredura partindo dos servidores da Paterva Online*
- *Você não consegue exportar seu projeto para outras extensões*

Varredura Passiva: Maltego

Na edição Comercial, você encontrará as seguintes opções:

- *Você pode usar para fins comerciais*
- *Não há limite de buscar por transform*
- *A comunicação entre cliente e servidor é através de SSL*
- *É executado através de um servidor muito mais potente*
- *As varreduras são compartilhada em servidores comerciais*
- *Suporte a usuário final*
- *Atualizações constantes*
- *Pode ser utilizado por qualquer servidor Maltego*

Varredura Passiva: Maltego

A função do Maltego é exercer um “data mining”, ou na melhor tradução, podemos dizer que ele faz um “garimpo de informações”.

A maior parte das atividades do Maltego poderiam ser realizadas a partir de scripts, buscas na web, consultas de DNS, etc.

O Maltego não explora diretamente nenhuma vulnerabilidade do objeto alvo de pesquisa. Sendo assim, podemos considerar que ele realiza varreduras não intrusivas, ou como costumamos chamar; varreduras passivas.

Não adianta utilizar esta ferramenta se você não traçar um objetivo ou linha de pesquisa, ou seja, não ter um alvo específico ou apenas procurar por pontos de falhas.

Será melhor aplicado se você obtiver um alvo, onde, nesse alvo, você explorar ou tentar explorar as pesquisas previamente adquiridas com a ferramenta.

Varredura Passiva: Maltego

Vamos antes, entender alguns conceitos.

Transforms: Devem ser pensados como pequenos pedaços de código com o objetivo de auxiliar o Maltego na sua mineração de dados.
Esses códigos podem se alterados para melhor apoia-lo em sua pesquisa, são geralmente desenvolvidos em Python ou PHP

TDS (Transform Distribution Server): É uma aplicação web que permite a distribuição e gestão de transformações, seeds e configurações. Essencialmente, o TDS significa que suas transformações são escritas como um serviço WEB (ou aplicações/páginas), e a TDS chamará esses scripts
Você pode obter acesso às TDSs através do link: https://cetas.paterva.com/TDS/
As TDSs podem ser públicas ou pagas, e por motivos óbvios, as melhores e úteis são as pagas.

Varredura Passiva: Maltego

Colocando em Prática

Acompanhe a vídeo aula

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker